DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Human Capital Services Center; Department of Veterans Affairs (VA).

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) proposes to establish a new system of records entitled VA Emergency Alerting and Accountability System (VA EAAS). The purpose is to document the enterprise-wide system used for alerting and accountability purposes. The system is a method to send rapid, reliable, and widespread notifications and collect the safety status of all VA employees, contractors, and affiliates in times of an emergency. The method provides situational leadership awareness of all personnel safety status, safety notifications to employees and provide actionable intelligence to leadership through data analysis and compilation.

DATES: Comments on this new system of records must be received no later than 30 days after the date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the new system of records will become effective a minimum of 30 days after the date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Ave. NW, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to “VA Emergency Alerting and Accountability System (VA EAAS) – VA (189VA006H)”. Comments received will be available at regulations.gov for public viewing, inspection, or copies.

FOR FURTHER INFORMATION CONTACT: For general questions about the system

contact Halena Lathe, Program Manager, Emergency Alerting and Accountability (EAAS) Program, Human Capital Services Center, (202) 632-4465 or VAEAASProgramOffice@va.gov.

SUPPLEMENTARY INFORMATION: VA Emergency Alerting and Accountability System (VA EAAS) is the replacement for the VA Notification System (VANS) system. The replacement VA EAAS system provides for improved accountability rates and increased usefulness across the enterprise to meet the needs of the Administrations, VA Medical Centers, VA Benefits Centers, National Cemeteries, and various VA offices throughout the nation. VA EAAS meets the requirement for a method to send rapid, reliable, and widespread notifications and collect the safety status of all VA employees, contractors, and affiliates in times of an emergency.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Neil C. Evans, M.D., Chief Officer, Connected Care, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on October 17, 2021 for publication.

Dated: November 18, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: VA Emergency Alerting and Accountability System (VA EAAS) – VA (189VA006H)

SECURITY CLASSIFICATION: Information in this SORN is not classified information.

SYSTEM LOCATION: The majority of the system is comprised of a BlackBerry vendor-hosted SaaS. The hosted SaaS performs all core functionalities of the system. There is a small component of the system that resides within the VA network. The User Synch Module resides in the VA Azure Enterprise Cloud platform. The component synchronizes VA Active Directory (AD) data to the hosted SaaS. The system is hosted on the Veterans Affairs (VA) Enterprise Cloud (EC), Microsoft Azure Government (MAG). The VA EC MAG is located in Azure Government Region 1 (USGOV VIRGINIA) and 2 (USGOV IOWA) and is designed to allow U.S. government agencies, contractors, and customers to move sensitive workloads into the cloud for addressing specific regulatory and compliance requirements.

SYSTEM MANAGER(S): Shannon E. Jones, Director, Human Capital Systems, Human Capital Services Center (HCSC), Department of Veterans Affairs (VA), 810 Vermont, Washington, DC 20420, 202-632-4465.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The authority which the system of records will be maintained includes:

(a) Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements. January 17, 2017.

(b) Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process, June 13, 2017.

(c) National Security and Homeland Security Presidential Directive (National Security Presidential Directive NSPD 51/Homeland Security Presidential Directive) HSPD-20, May 4, 2007.

(d) VA Directive 0320 VA Comprehensive Emergency Management Program, August 13, 2012.

(e) VA Handbook 0320 VA Comprehensive Emergency Management Program, March 24, 2005.

(f) VA Directive 0323 VA Continuity Program, November 5, 2010.

(g) VA Directive 0325 Department of Veterans Affairs Personnel Accountability, October 8, 2020.

PURPOSE(S) OF THE SYSTEM: The VA EAAS system enables the notification of incidents of an emergency nature to employees, contractors, affiliates and associates through multiple communication venues (e.g., email, cell phones, landline); generates reports of employees and contractors who have/have not responded; and allows designated personnel to monitor/manage select groups of employees/contractors.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: VA employees, contractors, or affiliates.

CATEGORIES OF RECORDS IN THE SYSTEM: The records will contain data on VA employees, contractors, or affiliates' name, VA email, work phone, home phone, personal cell phone, personal email, work address and home address.

RECORD SOURCE CATEGORIES: The information in this system of records is obtained from the following sources:

a. Information voluntarily submitted by VA employees, contractors, or affiliates.

b. Information extracted from the VA Active Directory (AD).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Routine use 1. Congress

VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

Routine use 2. Federal Agencies, for Research

"Routine Use 2 is used to allow the release of information for requests made by Federal Agencies, for Research." VA may disclose information to a Federal agency to conduct research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency.

Routine use 3. Data Breach Response and Remediation, for VA

VA may disclose information to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Routine use 4. Data Breach Response and Remediation, for Another Federal Agency

VA may disclose information to another Federal agency or Federal entity when VA determines that information from this system or records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations),

the Federal Government, or national security, resulting from a suspected or confirmed breach.

Routine use 5. DoJ for Litigation or Administrative Proceeding

VA may disclose information to the Department of Justice (DOJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

Routine use 6. Federal Agencies, Courts, Litigants, for Litigation or Administrative Proceedings

VA may disclose information to another federal agency, court, or party in litigation before a court or an administrative proceeding conducted by a Federal agency, when the government is a party to the judicial or administrative proceeding.

Routine use 7. Contractors

VA may disclose information to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

Routine use 8. OPM

VA may disclose information to the Office of Personnel Management (OPM) in connection with the application or effect of civil service laws, rules, regulations, or OPM guidelines in particular situations.

Routine use 9. EEOC

VA may disclose information to the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

Routine use 10. NARA

VA may disclose information to NARA in records management inspections conducted under 44 U.S.C. 2904 and 2906 or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

Routine use 11. Law Enforcement, for Locating Fugitive

In compliance with 38 U.S.C. § 5313B(d), VA may disclose information to any Federal, state, local, territorial, tribal, or foreign law enforcement agency to identify, locate, or report a known fugitive felon. If the disclosure is in response to a request from a law enforcement entity, the request must meet the requirements for a qualifying law enforcement request under the Privacy Act, 5 U.S.C. § 552a(b)(7).

Routine use 12. Unions

VA may disclose information identified in 5 U.S.C. § 7114(b)(4) to officials of labor organizations recognized under 5 U.S.C. Chapter 71, when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: VA EAAS is a BlackBerry vendor cloud-hosted Software as a Service (SaaS) solution. Data is

protected in accordance with FedRAMP/ National Institute of Standards and Technology (NIST) continuous monitoring guidance and controls.

System data is collected and maintained in an account created for each VA employee, facility-based contractor, and affiliate. The accounts and information will be kept secured in the VA EAAS databases as long as each person is working with VA. The information is maintained for personnel accountability and emergency notifications. Once the individual retires or separates from the Department, the listed information within their VA EAAS account will be stored for 30 days as a disabled account. If the individual's account is not reactivated within the 30 days, the account will be deleted permanently from the VA EAAS databases

Data backups will reside on appropriate media, according to normal system backup plans for VA Enterprise Operations. The system will be managed by VA HCSC, in VA Headquarters, Washington, DC.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by the names of the VA employee, contractor, or affiliate.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The information is maintained for personnel accountability and emergency notifications. Once the individual retires or separates from the Department, the listed information within their VA EAAS account will be stored for 30 days as a disabled account. If the individual's account is not reactivated within 30 days, the account will be deleted permanently from the VA EAAS databases.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The VA EAAS Operator or admin roles are necessary permissions to gain access. Each operator or admin must complete the required training to grant access. The accounts and information will be kept secured in the VA EAAS databases as long as each person is working with VA.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system of records may access the records via the Active Directory or submit a written request to the system manager.

CONTESTING RECORD PROCEDURES: An individual who wishes to contest records maintained under his or her name or other personal identifier may write or call the system manager. VA's rules for accessing records and contesting contents and appealing initial agency determinations are published in regulations set forth in the Code of Federal Regulations. See 38 CFR 1.577, 1.578.

NOTIFICATION PROCEDURES: Individuals wishing to inquire whether this system of records contains information about themselves should contact Human Capital Systems, Human Capital Services Center at (202) 632-4465 or VAEAASProgramOffice@va.gov.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: There are no exemptions for the system.

HISTORY: Not applicable; this is a new SORN.

[FR Doc. 2021-25509 Filed: 11/22/2021 8:45 am; Publication Date: 11/23/2021]